ADDITIONAL FEE:

Please charge any insufficiency of fee, or credit any excess, to Deposit Account No. 50-0427.

R E M A R K S

The Office Action issued June 20, 2005 has been received and its contents have been carefully considered.

Claim 18 has been rejected under 35 USC §112 and 35 USC §101. This claim has been amended to depend from claim 17, thus overcoming both informalities.

Claim 24 has also been amended to render it dependent from claim 37 and claim 25 has been canceled.

The Examiner has rejected applicant's claims 1-10, 17, 18 and 24-39 as being anticipated by Zampese U.S. Patent No. 6,014,650 ("Zampese"), and has rejected claims 11, 12, 14-16, 19, 20 and 21-23 as being unpatentable over Zampese. The Examiner also cites Franklin et al. U.S. Patent No. 6,000,832 ("Franklin"). These rejections are respectfully traversed for the reasons given below.

Although different in their implementation, Zampese's and Franklin's systems are very similar in their concept and functionality, both aiming to strengthen security for

passing the credit card information between customer, vendor and bank, specially through unreliable media (as with the internet).

Both patents propose the addition of a security code specific to each transaction and binding the effective use of such credit card to the validity of this additional code, and in this way rendering the credit card information insufficient for carrying out a transaction by itself and useless in case of interception by someone else.

In his patent, Zampese describes a simple, however effective, concept where the bank issuer of the card delivers to its customers (separately) a series of individual "secret codes" to be used, one in each transaction. The customer must include one secret code per transaction, enabling the bank to verify that a particular charge request from a vendor contained one of these "secret codes" it had previously given to the customer, and confirming in this way that the customer himself had requested the use of the credit card in such transaction. The code was also meant to be not reusable, guaranteeing that the information would be useless if intercepted.

By adding an additional requirement to the charge request, Zampese aimed to diminish the risk of a person

getting possession of someone else's credit card and performing a fraudulent transaction. In essence, Zampese provides an additional "per transaction security code" aimed to enhance security for transmitting credit card information over a network.

Franklin also implements a similar concept, but using software and encryption instead of pre-established codes. In his patent, he describes a system where the bank issues an "electronic" card and "software" capable of encrypting the electronic account together with the "per transaction security code". The software uses data pertaining to the customer, vendor and transaction itself to create an encrypted "number" that carries not only a reference to the account, but also this "security code" that is guaranteed to be unique to a particular transaction. As in Zampese's system, a person intercepting the data would not be able to use it since the validity of the information would be specific to that transaction alone.

In contrast, the "trigger system" according to the present invention is not a method for securing transmission of credit card information that an accountholder provides, mainly because in the trigger system, neither a credit card is being provided by the customer attempting the charge, nor

does the customer need to be necessarily the accountholder from which account funds will be ultimately withdrawn. On the contrary, the trigger system is a method for allowing someone to initiate a transaction without a credit card, with the intent of borrowing someone else's credit card from a separate institution not a party to the transaction.

This "borrowing" mechanism as described and claimed in this application occurs as a "separate borrowing transaction" altogether, outside of the sale/charge transaction between the vendor and the bank (where both the Zampese and Franklin systems reside).

In the Zampese and Franklin systems, the person starting the transaction is required to be the accountholder himself due to the need of supplying the credit card information (account) to the vendor in order to initiate the transaction. At no time does either Zampese or Franklin envision a system capable of starting a transaction without a credit card aiming to borrow this card in a separate transaction from an independent institution.

The fact that both Zampese and Franklin came up with different methods for securing the transmission of the credit card account information based upon secret codes is evidence that applicant's trigger system is not only novel

but "unobvious" to persons skilled in the art. These prior art methods are neither anticipatory nor suggestive of the borrowing/lending mechanism used by the trigger system which employs a secret code in order to start a transaction without an account (credit/debit card), aiming to borrow this account from someone else via a separate transaction performed by an independent institution not a party to the transaction.

There are several disadvantages of Zampese's and Franklin's systems when compared to the trigger system, starting with the fact that in both of these prior art systems, each bank would have to implement "their" version of the method (individually) in order to recognize the verification codes during charge requests, which could very well limit the widespread use of this functionality.

In the case of the trigger system, since the implementation occurs outside of the scope of the transaction, a single independent company implementing such "card borrowing" service can alone store and forward credit and debit cards to and from any other institution without any further involvement with the transactions in the accounts that participate in it.

In the end, the independent company works as a non-fiduciary participant in the transaction, whose only obligation to the transaction is to supply the credit/debit card information to this transaction assuming that the conditions for lending the use of the account are met.

It is important to understand that the trigger system is built around the fact that the service provider company responsible for lending the credit/debit cards is, on purpose, kept outside the universe of the transaction, excluding itself from any responsibility derived from the sale transaction. By doing so, it is capable of avoiding severe financial and regulatory burdens like anti-money laundering statutes, IRS controls, BSA (Bank Secrecy Act), OFAC (Office for Foreign Assets Control) and others.

Also, by not participating in the transaction itself, the service institution does not need to worry about accounts receivables from cardholders, accounts payables to vendor, charge disputes, refunds or any other issues related to the sale itself. These are burdens relegated to the parties participating in the transaction and are simply non-existent to the service provider since all it does is to supply credit/debit card information to transactions.

Cash flow issues are also of extreme importance when companies pay vendors in advance, financing customers from whom they expect to receive funds at a later time. These issues are also avoidable by using the trigger system due to its non-involvement with the sale transaction itself. As a result, the absence of so many financial and regulatory burdens translate into a very low operational cost and contribute to lower the prices of the service to the final consumer.

The trigger system allows for money transfer to occur directly between a cardholder and a beneficiary he/she chooses, by allowing the beneficiary to start a transaction without an account, presenting solely a borrowing code and withdrawing money directly from the accountholder's account without his/her participation or involvement in the transaction. These money transfer capabilities could have never been foreseen by Zampese or Franklin whose methods were only devoted to adding "extra" security to the transmission of credit card data.

As a specific example, the mother of applicant herein could punch a "secret code" at an ATM machine on the other side of the globe and, using the trigger system, "borrow/use" the applicant's credit card in order to

withdraw money from his account even though she is hundreds of miles away and has no relationship to applicant's account. For the ATM, it would be as if the applicant himself were there using his card, withdrawing the money and then giving it to her personally.

Neither Zampese nor Franklin's systems are capable of providing such benefits or avoiding the various problems mentioned above, since these systems merely apply added security to the transmission of credit card data passed between the parties involved in the transaction.

In his independent claim 1, Zampese claims a system where: "...a purchase request from a purchaser includes the purchaser's account code and a transaction code which has not been used before to prevent unauthorized purchases and fraud."

In Frankin's independent claim 39, he also recites the necessity of the account number in the purchase request when reciting the steps of: "embedding the code number in the customer account number" and "sending the customer account number with embedded code number to the merchant".

In the trigger system, the purchase request does not include the account information and the supplied code is actually used to acquire said credit card information from

the independent service provider, instead of serving as added security to the data being transmitted.

In the trigger system, the secret code is not used to mitigate concerns of transferring the credit card information between customer, vendor and bank, but as the borrowing mechanism for acquiring a credit card that was not supplied in the request for the transaction in the first place. To this end, applicant's independent claim 1 recites: "using an authorization code as a substitute for said account and the associated account approval information".

In both Zampese's and Franklin's systems, the "secret code" serves as a "per transaction validation" key used to legitimate the transaction that, without this code, would not be considered valid. In the trigger system, the "secret code" is the key for borrowing someone else's credit card information so that one can perform a purchase using someone else's credit card by supplying, instead of a credit card, a "borrowing" code.

Applicant's independent claim 1 further recites: "allowing either said terminal or host involved in said prospective credit or debit transaction to acquire said account and associated account approval information from a non-fiduciary external source..." and "...as if said account and

associated account approval information had been supplied to said external credit or debit transaction by the accountholder himself".

In his claim 4, Zampese recites the step of: "checking purchaser's account balance upon receiving a purchase request", which clearly implies that the institution implementing his system is the issuer of the card and the holder of the authority to approve the charge and commit itself to the payment to the vendor. This responsibility can be also found on Franklin's independent claim 39(c) where he recites the step of: "conducting a payment authorization phase at the issuing authority in response to receiving an authorization request from the merchant to honor the transaction number and accept payment..."

The trigger system does not receive a "purchase request" and does not commit itself to payments, but instead, it receives a request for borrowing someone else's credit card. Applicant's independent claim 1 recites: "delivers said account information and associated account approval information either to said terminal or host involved in said prospective credit or debit transaction in response to a request carrying an authorization code" and

also "in a request for acquiring said account and associated account approval information from the trigger server"

The trigger system cannot check the purchaser's account balance since the customer's balance belongs to the bank and the borrowing of the card occurs separately through the independent company not a party to the transaction (vendor/bank). Applicant's claim 1 further recites: "allowing either said terminal or host involved in said prospective credit or debit transaction to acquire said account and associated account approval information from a non-fiduciary external source, not a party to the transaction".

The Examiner mentions column 3, line 64, thru column 4, line 40, of the Zampese patent which states: "This purchase request includes purchaser's account code and a transaction code which has not been used before." In applicant's trigger system, the purchase request does not include any account, but instead an "authorization code" intended to borrow someone else's account (claim 1, sub-paragraph (c): "a requesting terminal...which receives an authorization code...as an alternate payment method for said credit or debit transaction")

In his independent claim 1 Zampese recites the step of "verifying that a purchase request from a purchaser includes the purchaser's account code and a transaction code", which explicitly dictates that the account number has to be provided during the request. Applicant's independent claim 1, in contrast, explicitly states that no account is submitted, but solely an authorization code "...as a substitute for said account and the associated account approval information".

Finally, Zampese clearly states in independent claim 1, that the account is supplied by the accountholder himself ("a purchase request from a purchaser includes the purchaser's account code") never envisioning the "cardless" request claimed by the trigger system where the purchase can be performed by someone other than the accountholder (applicant's independent claim 1: "enabling account withdrawals and charge requests to be initiated by either the accountholder himself or by someone other than the accountholder, using an authorization code as a substitute for said account and the associated account approval information" and "as if said account and associated account approval information had been supplied to said external credit or debit transaction by the accountholder himself".)

It is important to realize that, even though the trigger system does check that the conditions for borrowing such card are met, no relationship exists to the customer's account or account balance to the point that, if the card being borrowed is invalid or if there are insufficient funds in the account to approve the transaction being attempted, the trigger system simply would not know it.

Applicant's independent claims -- namely, apparatus claims 1, 31 and method claims 10, 37 -- as presently presented, clearly distinguish applicant's trigger system from the disclosures of Zampese and/or Franklin. These prior art references neither teach nor suggest the following elements or steps:

In Claim 1:

"...enabling account withdrawals and charge requests to be initiated by either the accountholder himself or by someone other than the accountholder, using an authorization code as a substitute for said account and the associated account approval information"

In Claim 1:

"allowing either said terminal or host involved in said prospective credit or debit transaction to acquire said account and associated account approval information from a non-fiduciary external source, not a party to the transaction and herein called a trigger server, outside of the boundaries of said credit or debit transaction and its associated parties, as if said account and associated account approval information had been supplied to at least one party to said transaction by the accountholder himself"

In Claim 1:

"...a trigger server which stores said account information, as well as said corresponding account approval information along with said account use restriction information, if any, in association with ~~a~~ an authorization code known to the accountholder, and thereafter delivers said account information and associated account approval information either to said terminal or host involved in said prospective credit or debit transaction in response to a request carrying an authorization code, provided that the verification of said authorization code is successful...".

In Claim 10:

"c) entering an authorization code at a requesting terminal, as an alternate payment method for said prospective credit or debit transaction between said terminal and a host;"

In Claim 10:

"f) the trigger server delivering to said terminal or host the account information and associated account approval information corresponding to said entered authorization code upon validation of said entered authorization code;

"g) the trigger server enabling said account and associated account approval information to be used as the charge or withdrawal account for said prospective credit or debit transaction between said terminal and host without further participating in any liability related to the outcome of said transaction; and

"h) allowing said credit or debit transaction attempt to occur between said terminal and host utilizing the acquired said account information and associated account approval information from said trigger server,

as if said account information and associated account approval information had been supplied to said credit or debit transaction by the accountholder himself."

In Claim 31:

"a) a computer server which receives, stores and delivers data defining a plurality of chargeable accounts for use in credit and debit transactions, as well as any additional information required for the effective use of said accounts, along with an authorization code associated with each account, said server being controlled by an institution which is not a party to said transactions..."

And in Claim 37:

"b) transmitting said data to a computer server controlled by an institution which is not a party to said transactions;

"c) said server confirming receiving and storing said data in association with a unique authorization code for each account;

"d) entering authorization codes at a requesting terminal;

"e) transmitting requests for acquiring said data to said server, utilizing said entered authorization codes; and

"f) said server validating said requests and delivering said data associated with said entered authorization code for use in said transactions, with no further involvement of said institution in said transactions."

Since the informalities noted by the Examiner have been overcome by this Amendment, and since all of the pending claims distinguish patentably over Zampese and Franklin for the reasons given above, this application is believed to be in condition for immediate allowance.

If the Examiner believes that a personal interview would be of value in resolving any remaining issues in this case, he is invited to telephone the undersigned counsel to arrange for such an interview.

Respectfully submitted,

By _____
Karl F. Milde, Jr.
Reg. No. 24,822

MILDE & HOFFBERG, LLP
10 Bank Street - Suite 460
White Plains, NY 10606

(914) 949-3100

I hereby certify that this correspondence is being deposited with the United States Postal Services as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on 8-12-05
MILDE & HOFFBERG, LLP
By _____
Date 8-12-05